

WHAT IS CLAIMED IS:

1. A method for dynamically managing access to a resource in a computer system, the system having a client thereof making an access request for the resource, the method comprising:

determining, via an application programming interface, based upon dynamic data and

5 first dynamic policy whether a client authorization context is to be updated, wherein said first dynamic policy is tailored to an application through which the resource is accessed;

identifying an access control entry as a callback access control entry; and

10 in response to identifying the access control entry as a callback access control entry, evaluating, via said application programming interface, based upon dynamic data and second dynamic policy whether said callback access control entry bears on said access request, wherein said second dynamic policy is tailored to said application.

2. A method according to claim 1, wherein said first dynamic policy defines flexible rules for determining the client authorization context and wherein said second dynamic policy defines
15 flexible rules for purposes of determining access privileges.

3. A method according to claim 1, further comprising computing the client authorization context after a request for a resource is received from the client and updating said client authorization context according to said determining.

4. A method according to claim 1, further comprising:
20 comparing the client authorization context of the client to at least one access control entry of an access control list.

5. A method according to claim 1, wherein said evaluating based upon dynamic data includes invoking an application-defined dynamic access check routine that performs based in
25 part upon dynamic data in the callback access control entry.

6. A method according to claim 5, wherein said access check routine is invoked automatically when there is a match between an identifier in the client authorization context and an identifier in the callback access control entry.

5

7. A method according to claim 1, further comprising registering with a resource manager, an application-defined routine for determining dynamic groups.

10

8. A method according to claim 1, further comprising registering with a resource manager, an application-defined routine for determining dynamic access checks.

9. A method according to claim 1, wherein said evaluating based upon dynamic data and second dynamic policy supplements a determination of access rights based upon static data and policy.

5

10. A computer readable medium having computer executable instructions for carrying out the method of claim 1.

20

11. A modulated data signal carrying computer executable instructions for performing the method of claim 1.

12. A computer readable medium having computer executable instructions stored thereon for carrying out a method for dynamically updating a client authorization context in a computer system, the method comprising:

25

computing a client authorization context after the request for the resource is received from the client;

determining, via an application programming interface, based upon dynamic data and

dynamic policy whether said client authorization context is to be updated, wherein said dynamic policy is tailored to an application through which the resource is accessed; and
 updating said client authorization context according to said determination.

5 13. A computer readable medium according to claim 12, the method further comprising:
 comparing the client authorization context to at least one access control entry of an access
 control list.

10 14. A computer readable medium according to claim 13, the method further comprising:
 identifying an access control entry as a callback access control entry.

15 15. A computer readable medium according to claim 14, further comprising:
 in response to identifying the access control entry as a callback access control entry,
 determining, via an application programming interface, based upon dynamic data and dynamic
 5 policy whether said callback access control entry bears on said access request, wherein said
 dynamic policy is tailored to said application.

20 16. A computer readable medium according to claim 15, wherein said determining based
 upon dynamic data includes invoking an application-defined dynamic access check routine that
 performs based in part upon dynamic data in the callback access control entry.

25 17. A computer readable medium according to claim 16, wherein said access check routine is
 invoked automatically when there is a match between an identifier in the client authorization
 context and an identifier the callback access control entry.

18. A computer readable medium according to claim 12, the method further comprising
 registering with a resource manager, an application-defined routine for determining dynamic

groups.

19. A computer readable medium according to claim 12, the method further comprising registering with a resource manager, an application-defined routine for determining dynamic access checks.

20. A computer readable medium according to claim 12, the method further comprising comparing data to a client authorization context determined based upon static data and policy before determining whether the client authorization context is to be updated.

21. A computer readable medium according to claim 15, wherein said determining based upon dynamic data whether said callback access control entry bears on said access request supplements a determination of access rights based upon static data and policy.

22. A computer readable medium bearing computer executable instruction for performing a method of dynamically managing access to a resource in a computer system, the system having a client thereof making an access request for the resource, the method comprising:

comparing the authorization context of the client to at least one access control entry of an access control list;

identifying an access control entry as a callback access control entry; and

in response to identifying the access control entry as a callback access control entry, determining, via an application programming interface, based upon dynamic data and dynamic policy whether said callback access control entry bears on said access request, wherein said dynamic policy is tailored to said application.

23. A computer readable medium according to claim 22, wherein said determining based upon dynamic data includes invoking an application-defined dynamic access check routine that

performs based in part upon dynamic data in the dynamic callback entry.

24. A computer readable medium according to claim 23, wherein said access check routine is invoked automatically when there is a match between an identifier in the client authorization context and an identifier the dynamic callback entry.

25. A computer readable medium according to claim 22, wherein said determining based upon dynamic data whether to grant the access request supplements a determination of access rights based upon static data and policy.

26. For an application in a computer system having a resource manager that manages and controls access to a resource, a computer readable medium bearing computer executable instruction for carrying out a dynamic authorization callback mechanism that provides extensible support for application-defined business rules via a set of APIs and DACLs including a dynamic groups element, which enables an application to assign temporary group membership, based on dynamic factors, to a client for the purpose of checking access rights

27. A computer readable medium bearing computer executable instruction for carrying out a dynamic authorization callback mechanism according to claim 26, further comprising a dynamic access check element, which enables an application to perform dynamic access checks, via DACLs and APIs, said dynamic access checks being customized to the application.

28. A computer readable medium bearing computer executable instruction for carrying out a dynamic authorization callback mechanism according to claim 26, wherein said dynamic groups element and said dynamic access element are registered with the resource manager upon initializing the resource manager.

29. A computer readable medium bearing computer executable instruction for carrying out a dynamic authorization callback mechanism according to claim 26, wherein said dynamic groups element and said dynamic access element utilize dynamic data that includes at least one of (1) data related to client operation, (2) authorization policy data stored in callback access control entry and (3) run-time data managed by the application.

30. A data structure stored on a computer readable medium for use in connection with dynamic access check determinations for an application in a computer system, the data structure comprising:

an identifier identifying the data structure as a callback access control entry; and
dynamic authorization policy data in a format tailored to the application.

31. A data structure according to claim 30, further comprising:
a security identifier.

32. A data structure according to claim 30, further comprising:
a list of access permissions.